REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
12-05-2014	Final Report	26-Aug-2009 - 25-Aug-2012

4. TITLE AND SUBTITLE
Final Report "Center for Quantum Algorithms and Complexity"

5a. CONTRACT NUMBER
W911NF-09-1-0440

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS
Umesh Vazirani

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of California - Berkeley
Sponsored Projects Office
2150 Shattuck Avenue, Suite 300
Berkeley, CA 94704 -5940

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
56295-PH-OC.12

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
How efficiently can the ground state of a local Hamiltonian be computed? This is a question that lies at the heart of an emerging area called "quantum Hamiltonian complexity", that addresses fundamental issues in both quantum complexity theory and condensed matter physics. Of particular importance are 1D Hamiltonians. We give a new combinatorial approach to proving the area law for 1D systems via the detectability lemma, in the process exponentially improving on Hastings' bounds in the frustration free case. We also give an efficient algorithm for finding an MPS approximation to the ground state, in the case of constant bond dimension.

15. SUBJECT TERMS
area law, detectability lemma, quantum PCP theorem

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Umesh Vazirani
UU	UU	UU	UU		19b. TELEPHONE NUMBER 510-642-0572

Report Title

Final Report "Center for Quantum Algorithms and Complexity"

ABSTRACT

How efficiently can the ground state of a local Hamiltonian be computed? This is a question that lies at the heart of an emerging area called "quantum Hamiltonian complexity", that addresses fundamental issues in both quantum complexity theory and condensed matter physics. Of particular importance are 1D Hamiltonians. We give a new combinatorial approach to proving the area law for 1D systems via the detectability lemma, in the process exponentially improving on Hastings' bounds in the frustration free case. We also give an efficient algorithm for finding an MPS approximation to the ground state, in the case of constant bond dimension.

Entanglement is a fundamental feature of quantum systems, and understanding its nature is a basic challenge in quantum computation.. We study it in a number of basic contexts, including the complexity of parallel repetition of entangled games, and Bell-inequalities distinguishing non-locality versus entanglement. We show how to use entanglement to give a way of generating certifiably random numbers which are provably secure even against a quantum adversary. The method is based on an earlier paper in which we report an implementation of optimal extractors against quantum storage.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received		Paper
04/17/2012	1.00	Dorit Aharonov, Itai Arad, Sandy Irani. Efficient algorithm for approximating one-dimensional ground states, Physical Review A, (07 2010): 0. doi: 10.1103/PhysRevA.82.012315
04/22/2012	3.00	Thomas Vidick, Stephanie Wehner. Does Ignorance of the Whole Imply Ignorance of the Parts? Large Violations of Noncontextuality in Quantum Theory, Physical Review Letters, (7 2011): 0. doi: 10.1103/PhysRevLett.107.030402
04/22/2012	2.00	Thomas Vidick, Stephanie Wehner. More nonlocality with less entanglement, Physical Review A, (5 2011): 0. doi: 10.1103/PhysRevA.83.052310
04/23/2012	7.00	Guoming Wang. Property testing of unitary operators, Physical Review A, (11 2011): 0. doi: 10.1103/PhysRevA.84.052328
04/27/2012	5.00	Dorit Aharonov, Itai Arad, Umesh Vazirani, Zeph Landau. The detectability lemma and its applications to quantum Hamiltonian complexity, New Journal of Physics, (11 2011): 0. doi: 10.1088/1367-2630/13/11/113043
05/12/2014	11.00	Itai Arad, Zeph Landau, Umesh Vazirani. Improved one-dimensional area law for frustration-free systems, Physical Review B, (5 2012): 0. doi: 10.1103/PhysRevB.85.195145
TOTAL:	**6**	

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received		Paper
04/22/2012	4.00	Julia Kempe, Thomas Vidick. Parallel repetition of entangled games, the 43rd annual ACM symposium. 05-JUN-11, San Jose, California, USA. : ,
04/22/2012	6.00	Dorit Aharonov, Lior Eldar. On the Complexity of Commuting Local Hamiltonians, and Tight Conditions for Topological Order in Such Systems, 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS). 21-OCT-11, Palm Springs, CA, USA. : ,
05/12/2014	8.00	Dorit Aharonov, Itai Arad, Zeph Landau, Umesh Vazirani. The 1D Area Law and the Complexity of Quantum States: A Combinatorial Approach, 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS). 22-OCT-11, Palm Springs, CA, USA. : ,
05/12/2014	9.00	Umesh Vazirani, Thomas Vidick. Certifiable quantum dice, the 44th symposium. 18-MAY-12, New York, New York, USA. : ,
05/12/2014	10.00	Anindya De, Thomas Vidick. Near-optimal extractors against quantum storage, the 42nd ACM symposium. 04-JUN-10, Cambridge, Massachusetts, USA. : ,
TOTAL:	**5**	

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper
TOTAL:	

Number of Manuscripts:

Books

Received Paper

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Thomas Vidick	0.10	
Anupam Prakash	0.15	
Urmila Mahadev	0.05	
Guoming Wang	0.20	
Seung Woo Shin	0.10	
FTE Equivalent:	**0.60**	
Total Number:	**5**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Falk Unger	0.50
Yi-Kai Liu	0.10
Andre Chailloux	0.30
FTE Equivalent:	**0.90**
Total Number:	**3**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Umesh Vazirani	0.10	No
FTE Equivalent:	**0.10**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):.....	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME
Thomas Vidick

Total Number: **1**

Names of other research staff

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

1 a. Hebrew University of Jerusalem

1 b. Authority for Research & Developm
The Sherman Building for Research
Givat Ram, Jerusalem a 91904

Sub Contractor Numbers (c):
Patent Clause Number (d-1):
Patent Date (d-2):
Work Description (e):
Sub Contract Award Date (f-1):
Sub Contract Est Completion Date(f-2):

Inventions (DD882)

Scientific Progress

Technology Transfer

Final report on ARO Proposal Number 56295PHQC: "Center For Quantum Algorithms and Complexity"

Umesh Vazirani

1 Introduction:

Quantum Hamiltonian Complexity (QHC) is an emerging area that combines deep questions and techniques from both quantum complexity theory and condensed matter physics. It also provides some of the basic theory to support the major effort in condensed matter physics to explore highly entangled states of matter. At the heart of QHC is the striking feature of quantum systems — one of the great challenges posed by the laws of quantum mechanics is that the complexity of quantum systems grows exponentially in the number of particles, making it prohibitively hard to classically simulate or even understand them. Is it possible that "typical" quantum systems occurring in Nature do not suffer this exponential overhead (after all if this were not the case, how is it possible to do physics)?

Remarkably, these questions are intimately related to the most basic questions in computational complexity theory, namely the complexity of constraint satisfaction problems. A deep insight from condensed matter physics is the area law for gapped Hamiltonians. This sweeping conjecture in condensed matter physics, called the *area law*, asserts that gapped Hamiltonians have limited entanglement in their ground states. More precisely, it asserts that for any subset L of particles, the entanglement entropy between L and $\bar{L}$ is bounded by the surface area of L (the area is measured by the number of terms of the Hamiltonian H that cross between L and $\bar{L}$), rather than (the trivial bound of) the volume of L(see Figure 1). Intuitively, the area law suggests that most of the entanglement in the ground state is local; indeed if this were true in a precise sense then the ground state would have a succinct classical description. In a seminal paper, Hastings proved that ground states of gapped 1D systems obey an area law. We give a new combinatorial approach to proving the area law for 1D systems via the detectability lemma, in the process exponentially improving on Hastings' bounds in the frustration free case [2,3,4].

The heuristic DMRG has been an invaluable practical tool for solving 1D quantum systems every since its introduction about two decades ago. But there is no proof of when it works. We give an efficient algorithm for finding an MPS approximation to the ground state, in the case that it can be approximated by a Matrix Product State (MPS) with constant bond dimension [5].

Entanglement is a fundamental feature of quantum systems, and understanding its nature is a basic challenge in quantum computation. We study it in a number of basic contexts, including the complexity of parallel repetition of entangled games [6], and Bell-inequalities distinguishing non-locality versus entanglement [7].

A source of independent random bits is a basic resource in many modern-day computational tasks, such as cryptography, game theoretic protocols, algorithms and physical simulations. Moreover, these tasks place different demands on the quality of the randomness (e.g. the need for privacy in cryptographic applications). It is of great interest, therefore, to construct a physical device for reliably and provably outputting a stream of random bits. But suppose even that such a device were built: how could one verify that the generated bits are indeed random? Testing for the the production of uniformly random bits poses a fundamental problem — since all outputs should be generated with equal probability there is no basis for rejecting any particular output of the device. We show how to use entanglement to give a way of generating certifiably random numbers which are provably secure even against a quantum adversary [9]. The method is based on an earlier paper in which we report an implementation of optimal extractors against quantum storage [8].

2 Scientific Progress:

Quantum Hamiltonian Complexity:

How efficiently can the ground state of a local Hamiltonian be computed? This is a question that lies at the heart of an emerging area called "quantum Hamiltonian complexity", that addresses fundamental issues in both quantum complexity theory and condensed matter physics. Ground states of quantum many-body systems on a lattice, which are ubiquitous in condensed-matter physics, provide a natural setting to explore this question. These systems are generally described by a local Hamiltonian that models interactions between neighboring particles. A remarkable conjecture in condensed-matter physics dating back about a half century is the Area Law, which strongly bounds the entanglement in ground states of gapped local Hamiltonians. Roughly, it says that the entanglement in such states is very local, and the entanglement entropy scales like surface area rather than volume of any region. In a seminal paper (Hastings 2007 J. Stat. Mech. (2007) P8024), Hastings proved that ground states of gapped 1D systems obey an area law. More specifically, if the dimension of each particle is d, and the spectral gap of the Hamiltonian is ?, then the theorem states that the entanglement entropy is bounded by $exp(X)$, where $X = log(d/?)$. Hastingss result implies that ground states of gapped 1D systems can be well-approximated by a polynomial size tensor network (MPS), which can in turn be used to approximate any local observable efficiently on a classical computer.

In [2], we focus on a seemingly specialized technical tool, the detectability lemma (DL), introduced in the context of the quantum PCP challenge [1], which is a major open question in quantum Hamiltonian complexity. We show that a reformulated version of the lemma is a versatile tool that can be used in place of the celebrated LiebRobinson (LR) bound to prove several important results in quantum Hamiltonian complexity. The resulting proofs are much simpler, more combinatorial and provide a plausible path toward tackling some fundamental open questions in Hamiltonian complexity. We provide an alternative simpler proof of the DL that removes a key restriction in the original statement [1], making it more suitable for the broader context of quantum Hamiltonian complexity. Specifically, we apply the DL to derive a simpler and more intuitive proof of Hastings' seminal one-dimensional (1D) area law (Hastings 2007 J. Stat. Mech. (2007) P8024) (the proofs are restricted to frustration-free systems). Proving the area law for two and higher dimensions is one of the most important open questions in the field of Hamiltonian complexity, and the combinatorial nature of the DL-based proof holds out hope for a possible generalization. Finally, we also provide a more general explanation of how the DL can be used to replace the LR bound.

In a sequence of follow-up papers, we have improved Hastingss bound by an exponential factor for frustration-free Hamiltonians [3,4]. Ignoring lower-order terms, the new bound on entanglement entropy is $O(X^3)$. The proof uses completely new techniques, including a new bootstrapping technique for finding a product state with large overlap with the ground state, and combinatorial tools such as Chebyshev polynomials to construct an Approximate Ground State Projector. These results leave us at the threshold of being able to tackle three fundamental issues. First, in terms of dealing with systems of dimension greater than 1, the new techniques can be used in conjunction with simple locality considerations to show an entanglement entropy bound of $O(Area^2)$. While this stops just short of giving a non-trivial bound for 2D systems, it does give a sub-volume law for any system of fractal dimension ¡ 2. Extending these results to 2D systems is a central problem in this field, and is awaiting a better technique for incorporating the locality of the Hamiltonian along the cut. Second, the new proof also gives very strong upper bounds for the Schmidt coefficients of the ground state. For 1D systems these bounds can be used to construct much smaller tensor network (MPS) representations of these states. Finally, these techniques should be strengthened to deal with general, frustrated systems.

The area law results show that the ground state of a 1D system can be well approximated by a

succinct classical description in the form of a Matrix Product State (MPS). How hard is it to find such an approximating MPS? The DMRG method is very effective at finding ground states of 1D quantum systems in practice, but it is a heuristic method, and there is no known proof for when it works. In [5] we describe an efficient classical algorithm which provably finds a good approximation of the ground state of 1D systems under well defined conditions. More precisely, our algorithm finds a Matrix Product State of bond dimension D whose energy approximates the minimal energy such states can achieve. The running time is exponential in D, and so the algorithm can be considered tractable even for D which is logarithmic in the size of the chain. The result also implies trivially that the ground state of any local commuting Hamiltonian in 1D can be approximated efficiently; we improve this to an exact algorithm.

Quantum Entanglement:

In [6], we consider one-round games between a classical referee and two players. One of the main questions in this area is the parallel repetition question: Is there a way to decrease the maximum winning probability of a game without increasing the number of rounds or the number of players? Classically, efforts to resolve this question, open for many years, have culminated in Raz's celebrated parallel repetition theorem on one hand, and in efficient product testers for PCPs on the other. In the case where players share entanglement, the only previously known results are for special cases of games, and are based on techniques that seem inherently limited. Here we show for the first time that the maximum success probability of entangled games can be reduced through parallel repetition, provided it was not initially 1. Our proof is inspired by a seminal result of Feige and Kilian in the context of classical two-prover one-round interactive proofs. One of the main components in our proof is an orthogonalization lemma for operators, which might be of independent interest.

In [7], we provide an explicit example of a Bell inequality with 3 settings and 2 outcomes per site for which the largest violation is not obtained by the maximally entangled state, even if its dimension is allowed to be arbitrarily large. This complements recent results by Junge and Palazuelos (arXiv:1007.3042) who show, employing tools from operator space theory, that such inequalities do exist. Our elementary example provides arguably the simplest setting in which it can be demonstrated that even an infinite supply of EPR pairs is not the strongest possible nonlocal resource.

Quantum Random Number Generation:

A source of independent random bits is a basic resource in many modern-day computational tasks, such as cryptography, game theoretic protocols, algorithms and physical simulations. Any attempt to actually build a physical device to generate random bit sequences runs into a fundamental problem: how do you test whether the output is really random. In other words, since all outputs should be generated with equal probability there is no basis for rejecting any particular output of the device.

Quantum mechanics allows for a remarkable random number generator: its output is certifiably random in the sense that if the output passes a simple statistical test, and there is no information communicated between the two boxes in the randomness generating device (based, say, on the speed of light limit imposed by special relativity), then the output is certifiably random. Moreover, the proof that the output is truly random does not even depend upon the correctness of quantum mechanics!

This is based on a remarkable line of work inspired by device independent quantum cryptography, starting with an observation in Colbeck's Phd thesis, and further developed in a paper by Pironio et. al. to give a scheme which certifiably expanded $\sqrt{n}$ random bits to n random bits. There were two major issues left open. The first was whether the expansion factor could be made exponential rather than polynomial. Even more important was the question of whether the randomness certification could be guaranteed against a quantum adversary. i.e. if the devices were manufactured by an adversary

who can make use of quantum phenomena like entanglement.

In [9], we gave resolved both issues. We gave a protocol through which a pair of quantum mechanical devices may be used to generate n bits of true randomness from a seed of $O(\log n)$ uniform bits. The bits generated are certifiably random based only on a simple statistical test that can be performed by the user, and on the assumption that the devices obey the no-signaling principle. No other assumptions are placed on the devices' inner workings. A modified protocol uses a seed of $O(\log^3 n)$ uniformly random bits to generate n bits of true randomness even conditioned on the state of a quantum adversary who may have had prior access to the devices, and may be entangled with them.

The proof of security is quite non-trivial and is based on the security of Trevisan's extractor against quantum adversaries, which is also reported here [8]. We show that Trevisan's extractor and its variants are secure against bounded quantum storage adversaries. One instantiation gives the first such extractor to achieve an output length $\Theta(K - b)$, where K is the source's entropy and b the adversary's storage, together with a poly-logarithmic seed length. Another instantiation achieves a logarithmic key length, with a slightly smaller output length $\Theta((K-b)/K\gamma)$ for any $\gamma > 0$. In contrast, the previous best construction could only extract $(K/b)^{1/15}$ bits. Some of our constructions have the additional advantage that every bit of the output is a function of only a polylogarithmic number of bits from the source, which is crucial for some cryptographic applications. Our argument is based on bounds for a generalization of quantum random access codes, which we call *quantum functional access codes*. This is crucial as it lets us avoid the local list-decoding algorithm central to previous approaches, which was the source of the multiplicative overhead.

Bibliography:

[1] Aharonov, D., Arad, I., Landau, Z., and Vazirani, U. The detectability lemma and quantum gap amplification. In Proceedings of the 41st Annual ACM Symposium on theory of Computing (Bethesda, MD, USA, May 31 - June 02, 2009). STOC '09. ACM, New York, NY, 417-426.

[2] Aharonov, D., Arad, I., Landau, Z., and Vazirani, U. The 1D Area Law and the Complexity of Quantum States: A combinatorial approach. Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (2011).

[3] Aharonov, D., Arad, I., Landau, Z., and Vazirani, U. The detectability lemma and its applications to Quantum Hamiltonian complexity. New J. Phys. 13 (2011).

[4] I.Arad, Z.Landau, U. Vazirani. An improved 1D area law for frustration-free systems. Phys. Rev. B 85, 195145 (2012).

[5] Aharonov, D., Arad, I., Irani, S. Efficient algorithm for approximating one-dimensional ground states Phys. Rev. A 82, 012315 (2010).

[6] J. Kempe, T. Vidick. Parallel Repetition of Entangled Games. STOC'11.

[7] T. Vidick, S. Wehner. More non-locality with less entanglement. Phys. Rev. A 83, 052310 (2011).

[8] A. De, T. Vidick. Near-optimal extractors against quantum storage. STOC'10.

[9] T. Vidick, U. Vazirani. Certifiable Quantum Dice: or, true random number generation secure against quantum adversaries. Proceedings of the ACM Symposium on the Theory of Computing (2012).